Vulnerability Assessment & Remediation Management Integration (VARMINT)

Phase I – Proof of Concept of BigFix on sample of 15-30 servers at VDC for discovery purposes only (action capability turned off) and to assess threat exposure, define and assign impact levels and create policies. Also establish manual workflow procedures and responsibilities. NOTE: This does nothing to effect any commitment to a specific product. Full use of BigFix is provided on a trial basis for up to 60 days.

Phase II – Enable CSC personnel to utilize BIGFix remediation features if desired or enforce use if their existing methods are not able to keep up with demands.

Phase III – Extend to rest of VDC

Phase IV – Extend to CSB

Phase V - Automate workflow and accountability

Phase VI – Integrate other vulnerability detection and remediation tool(s) for network devices, etc.

Phase VII – Extend to TSYS/FEBI

Phase VIII – Extend solution to EdNet other POC's

Phase I - Proof of Concept	Costs

Objective: To establish value of centralized monitoring, knowledge of inventory, vulnerability exposure, and automated vulnerability and patch management remediation processes and tasks.

    a. Description
A Windows 2000 Server will reside on the tenth floor at FSA running BigFix Enterprise Server Software. Approximately 15 servers $_____

    b. Define roles, responsibilities
    c. Coordinate contractor relationships
    d. Implementation Requirements
        i. Obtain Hardware…………………………………………………………………

- *BES Server* - One P1Gz+ Server w/ 512mb ram, 40GB HDD, 512mb ram MS 2000 Server, NIC, and KVM residing at FSA $_____
- *Relay* - One PIII+, 1+Gz Server w/ 512mb ram, 40GB HDD, 512mb ram, NIC, MS 2000 Server and KVM residing at VDC (alternative is sharing underutilized existing MS2000 Server at VDC)   60 Day Trial

        ii. Arrange Communications…………………………………………………………. $_____
- EDNet private network

        iii. Acquire Software………………………………………………………………….. $_____
- BigFix Enterprise Server, Relay, and 15 Agent licenses

        iv. Install Personnel
…………………………………………………………………………………..

        v. Obtain CSC Services……………………………………………………………….
- VDC Firewall and other network changes
- Agent installation facilitation $_____
- Any change management doc work resulting
- Set up of Relay server or installation of relay software on existing box $_____
- Other

        vi. Obtain Major App Contractor Services…………..…………..………..………..

        vii. Provide BearingPoint Services (as function of current contract)…………………

➤ Perform Training	$_____
➤ Perform Evaluation, Risk Assessment, and Remediation Planning	
➤ Action Response Procedure Development	
➤ Workflow and Responsibility Development	